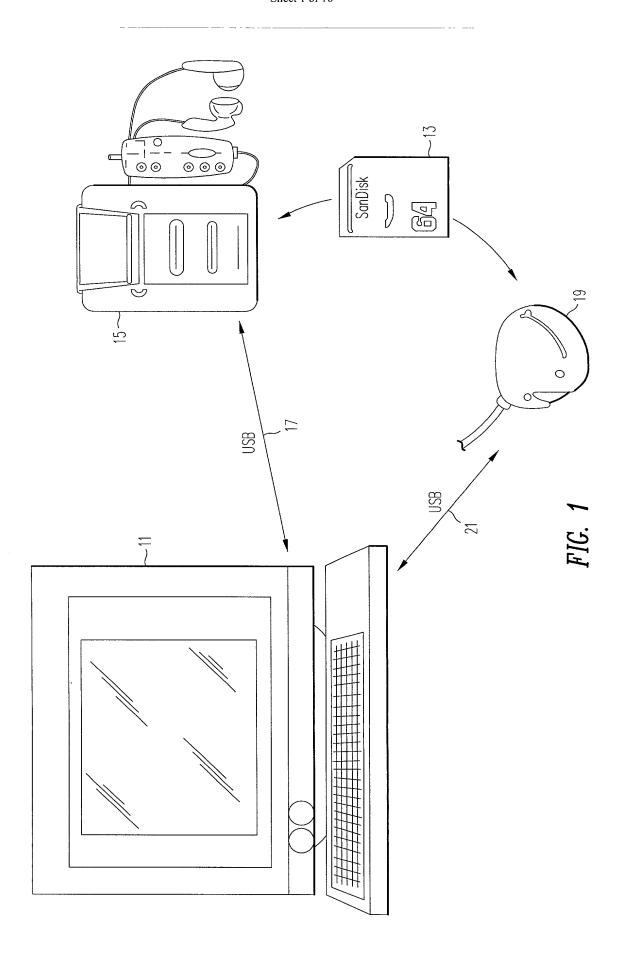
Inventors: Sabet-Sharghi et al. Atty. Dkt. No M-9913 US Sheet 1 of 16



Inventors: Sabet-Sharghi et al Atty. Dkt No M-9913 US Sheet 2 of 16

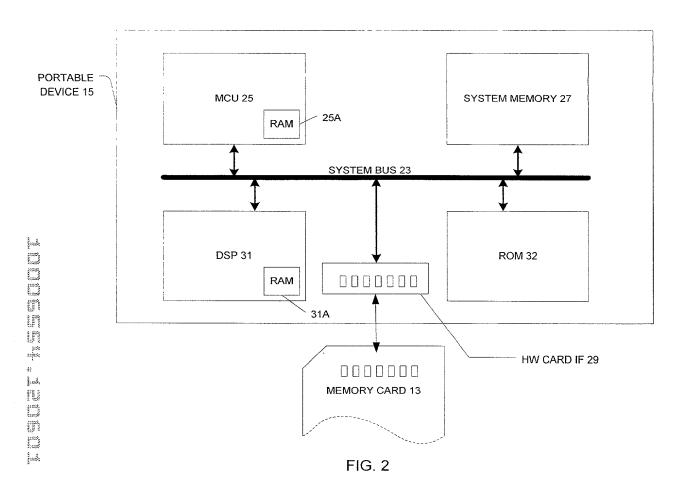
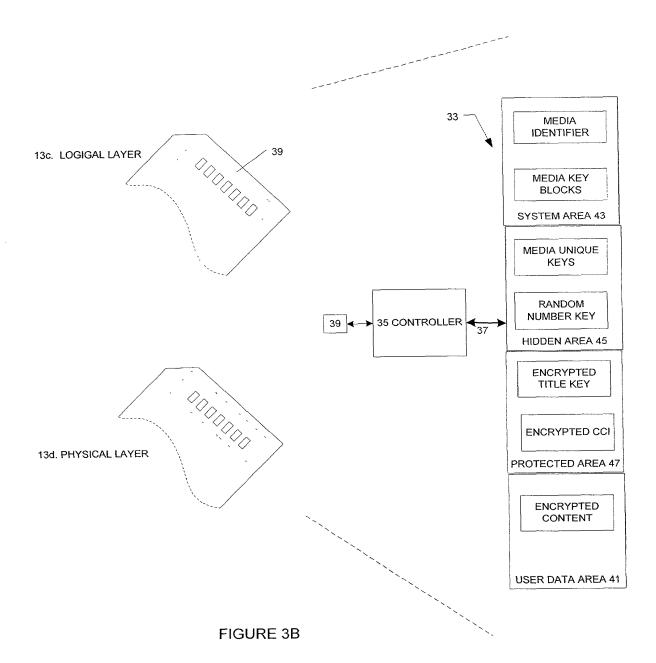
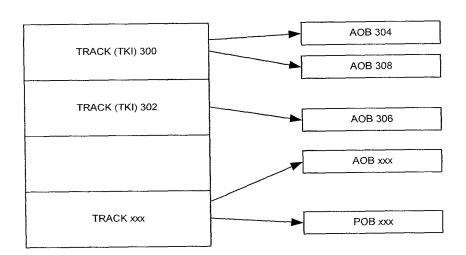


FIGURE 3A

requests for content and keys received DEVICE **INTERFACE 39** ELECTRICAL encrypted content and CONTACTS encrytped keys to decrypt content transmitted 13a. APPLICATION LAYER communicates with device accessing content 13b. SECURITY LAYER controls access to logical and physical layers 0000000 MEMORY CARD 13 13c LOGIGAL LAYER files, tracks, directory structure of content corresponding to clusters, AND encrypted keys 13d PHYSICAL LAYER clusters of memory cells 33 with encrypted content and keys

Inventors: Sabet-Sharghi et al. Atty. Dkt. No. M-9913 US Sheet 4 of 16





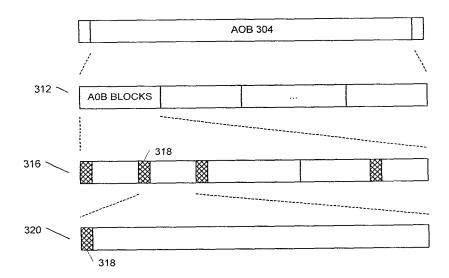
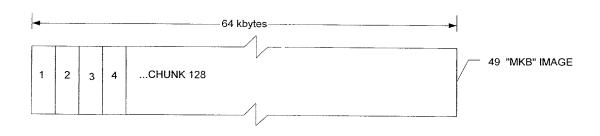


FIG. 3C

Inventors: Sabet-Sharghi et al. Atty. Dkt. No. M-9913 US Sheet 6 of 16



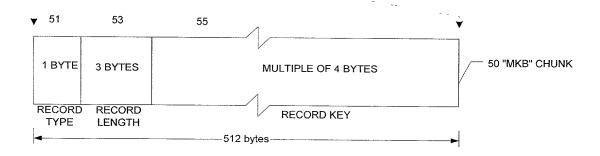


FIG. 4

Sheet 7 of 16

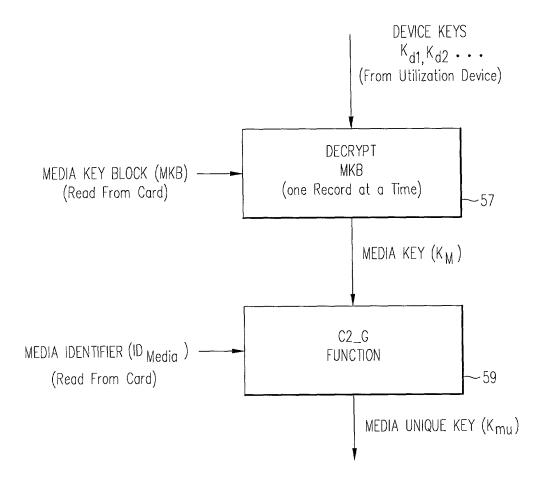


FIG. 5

Sheet 8 of 16

CCI Out (least significant 56-bits of 64 bits output) Content Out 56 × K+ 9 Device Keys In (K<sub>d1,</sub>K<sub>d2,...,</sub>K<sub>d16</sub>) -59 57 FIG. DCBC Ы  $C2_D$ 77,  $C_{1}^{2}$ 9 (1)Process\_MKB  $(2)C2_{-}$ Kmu 🕇 ,69 .83, 65 79, DCBC Ks. (3)AKE 45 <u>,</u> ∑ 4 Ks C2\_ ECBC **Encrypted Content** Memory Card Protected Area User Data Area System Area Hidden Area ID media K<sub>te</sub>llenc -CCI Kmu MKB DCBC Ks  $\infty$ (3)AKE C2\_ ECBC (1)Process\_MKB 73 . Kmu 63 ی Device Keys In (K<sub>d1,</sub>K<sub>d2,...,</sub>K<sub>d16</sub>) 83  $(2)C2_{-}$ (least significant 56—bits ' of 64 bits output) X M 69  $C_2$ ECBC 59, 57,  $C_{2}$ CCIContent In ⊼ + **6**7 Keys In (4) (5)

Sheet 9 of 16

Pick up the argument RN Generator (C2\_G) Challenge1 - Challenge2 Memory Card  $C2\_G$  $C2_6$ Media Unique Key (K<sub>mu</sub>) Bitwise Compliment  $C2_{6}$ Session Key Verify Challenge2 Challenge1 Response1 Response2 FIG. 7 Media Unique Key (K<sub>mu</sub>) Verify Session Key Bitwise Compliment 0.02 - 0.00 $0.2_{-6}$  $C2_6$ (MSB) (LSB) Secured Command RN Generator (C2\_G) Argument of Challenge1 -Challenge2

The first control of the first by the first beautiful to the first by the first by

Inventors: Sabet-Sharghi et al. Atty. Dkt. No. M-9913 US Sheet 10 of 16

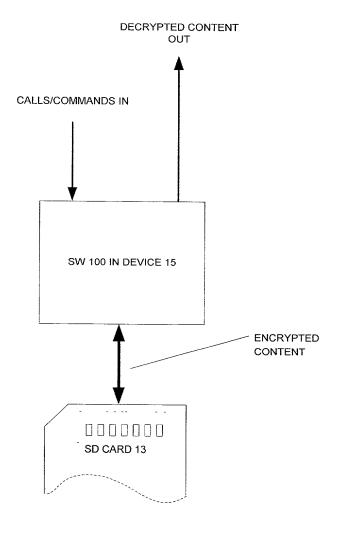
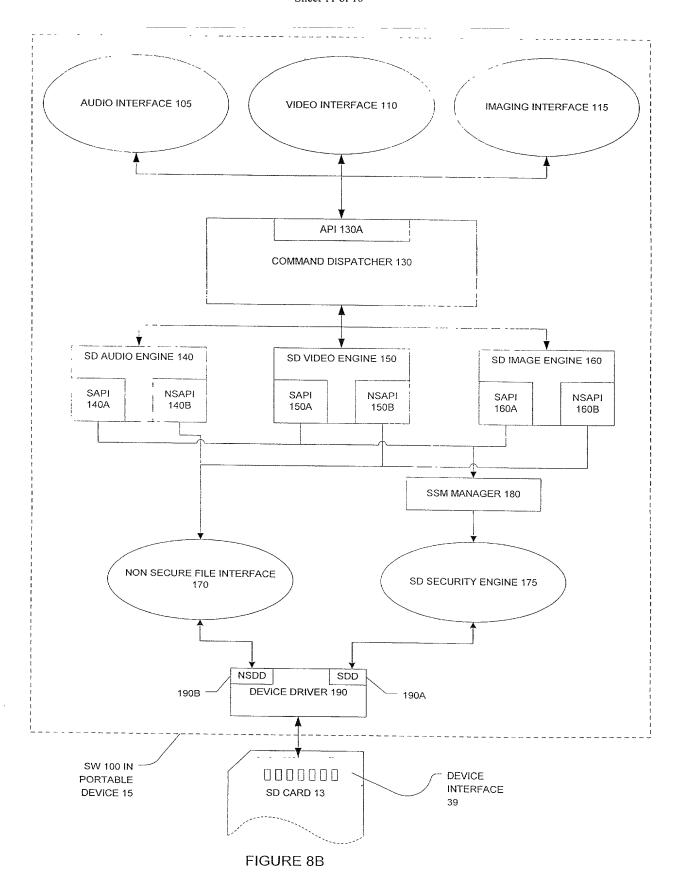


FIG 8A

Inventors: Sabet-Sharghi et al. Atty. Dkt. No. M-9913 US Sheet 11 of 16



Inventors: Sabet-Sharghi et al. Atty. Dkt. No. M-9913 US Sheet 12 of 16

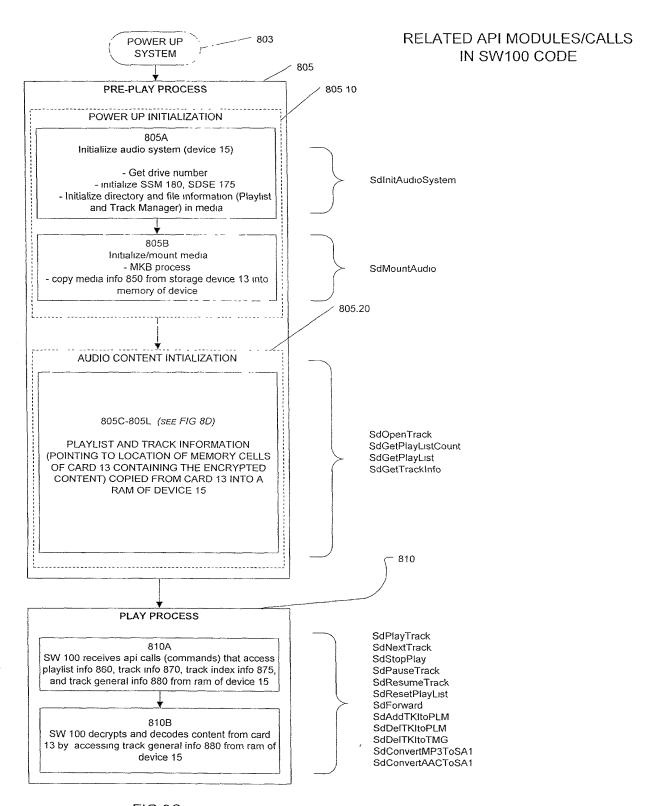
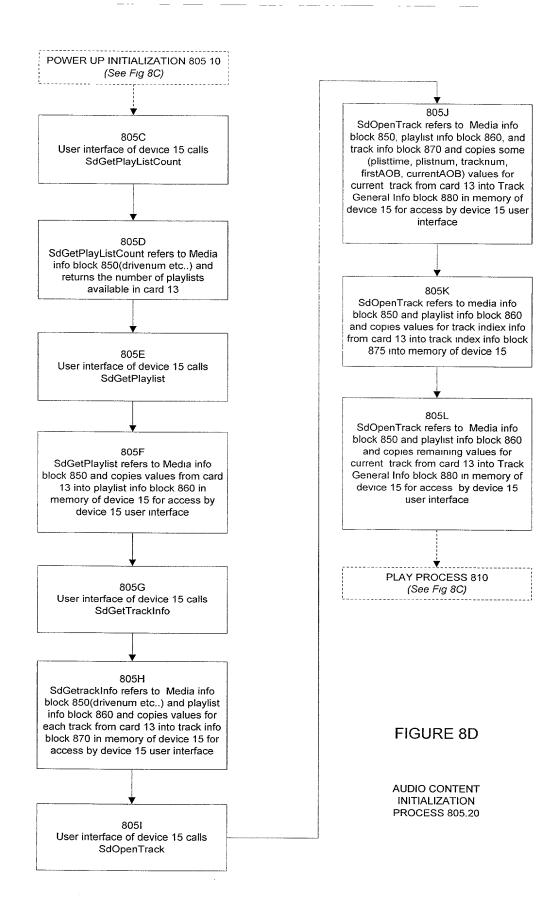


FIG 8C

Inventors: Sabet-Sharghi et al. At Sheet 13 of 16

Atty. Dkt. No. M-9913 US



plistn um

fdAOB

Track Gen Info SanDisk cmd audioformat Media Info 880 sampfreq pTGInfo 850 appAttrib SanDisk **sizeAOB** drivenum currentAOB security firstAOB **lastAOB** mounted countAOB syneword Track Info seekposAOB trackTime trkElapsedTime bytesize trackTime tkisInTrack bytesize 875 elementplaytime tracknum Track Index Info tracknum index trackTime **fwTime** trkInformation[...] seekpos fwNext bytesize tracksInPlist aobsize pListTime **Playlist Info** 860 elementsize audio\_attribute pListTime elementoffset app\_attrib tracksInPlist currentelement tkicount index totalelements lastTKI Length

> PRE-PLAY STRUCTURES FIG 8E

elementplaytime

pListName[...]

205 PROCESS MKB IMAGE **CORRESPONDING API** IN CODE MKB -> Km -> Kmu **PARTIALLY** PROCESS AKE SEC\_AKE API Kmu -> Ks SEC\_ENC\_TKEY API DELETE Kmu USE SESION KEY (Ks) TO DECRYPT DOUBLY 215 **ENCRYPTED TITLE KEY**  $E(E(Kt)) \rightarrow E(Kt)$ STORE E(Kt) IN A MEMORY OF THE DEVICE 225 READ PORTION OF TRACK 225a CALCULATE Kmu DECRYPT E(Kt) 225b  $E(Kt) \rightarrow Kt$ SEC\_DEC\_TKEY API NO USE Kt TO SEC\_GETCCI API ~ DECRYPT 225c CONTENT OF SEC\_UPDATECCI API BUFFER **DELETE Kt** 225d DELETE Kmu 225e ALL PORTIONS OF TRACK READ? 235

FIGURE 9

NEXT TRACK

Inventors: Sabet-Sharghi et al. Atty. Dkt. No. M-9913 US Sheet 16 of 16

